

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **GD0-100**

Title : Certification Exam For
ENCE North America

Version : Demo

1. When an EnCase user double-clicks on a file within EnCase what determines the action that will result?

Select all that apply

- A. The settings in the case file.
- B. The settings in the FileTypes.ini file.
- C. The setting in the evidence file.

Answer: B

2. Search results are found in which of the following files? Select all that apply.

- A. The evidence file
- B. The configuration Searches.ini file
- C. The case file

Answer: C

3. If cluster #3552 entry in the FAT table contains a value of this would mean:

- A. The cluster is unallocated
- B. The cluster is the end of a file
- C. The cluster is allocated
- D. The cluster is marked bad

Answer: A

4. The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result.

Bob@ [a-z]+.com

- A. Bob@New zealand.com
- B. Bob@My-Email.com
- C. Bob@America.com
- D. Bob@a-z.com

Answer: C

5. You are an investigator and have encountered a computer that is running at the home of a suspect. The computer does not appear to be a part of a network. The operating system is Windows XP Home. No programs are visibly running. You should:

- A. Pull the plug from the back of the computer.
- B. Turn it off with the power button.
- C. Pull the plug from the wall.
- D. Shut it down with the start menu.

Answer: A